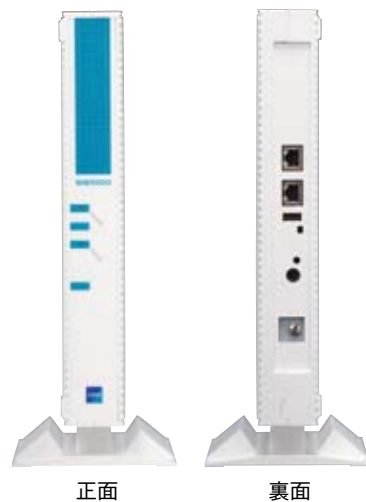
■主な機能

- ●ファイアウォール
- ●ウイルスブロック(ヒューリスティック検知対応)
- ●スマートフォン(Android用パッケージファイル)のウイルス検知対応
- ●URLフィルタリング
- ●Webアンチウイルス(HTTPフルスキャン)
- ●IDP(侵入検知・防止)
- ●迷惑メールブロック
- ●P2P/メッセンジャーソフト対策(Winnyなどに対応)
- ●ルータ機能搭載
- ●VPN対応
- ●ウイルス/スパム定義ファイル自動更新
- ●自動ファームアップ

■主な仕様

項目	仕様
本体寸法(mm)	210(W)×47(H)×297(D)
重量(kg)	1.6
環境温度	0~40℃
相対湿度	90%以下
電圧/周波数	DC12V
最大消費電力	24VA
EMI/安全基準/認証	日本:VCCI-A、JATE
推奨接続台数	20台
インターフェース	USB2.0 LAN:10/100/1000Mbps WAN:10/100/1000Mbps
付属品	ACアダプタ
オプション品	据置用品(スタンド)/壁掛用品

正面　裏面

Ahkun AntiMalware-AV
エンドポイントセキュリティ動作環境

Ahkun

クライアントプログラム動作環境	OS	Windows 7/Vista/XP、Windows Server 2008、2003 32bit/64bit
	CPU	Intel Pentium4 1.3GHz相当以上
	メモリ空き容量	256MB以上
	ディスク空き容量	インストール時に300MB以上
	WEB環境	Internet Explorer 7.0以上 [注意事項]マシンへのログオン時のみ、すべての機能が利用可能です。 マシン速度、環境により十分なパフォーマンスが発揮できない場合があります。
管理マネージャー動作環境	WEB環境	Internet Explorer 7.0以上
	画面解像度	1,024×768以上

安全に関するご注意

●本商品ご購入後は、添付の「取扱説明書」をよくお読みの上、正しくお使いください。「取扱説明書」には、本商品をご購入されたお客さまや他の方々への危害や財産の損害を未然に防ぎ、本商品を安全にお使いいただくために守っていただきたい事項を記載しています。
●水、湿気、湯気、ほこり、油煙などの多い場所には設置しないでください。火災、感電、故障などの原因となることがあります。

〔本体について〕●本製品はネットワーク上の脅威に対してそのリスクを低減させるための装置です。本製品を導入することによりその脅威を完全に取り除くことを保障するものではありません。●お客様の環境により別途HUBが必要な場合があります。●各種セキュリティ機能の有効期限は使用開始から5年間、SS1000α Plusは6年間となります。5年(6年)が経過すると各種セキュリティ機能は無効となり、脅威の防御効果が著しく減少してしまいますのでご注意ください。●本製品に多くのトラフィック負荷がかかると、回線速度が低下する場合がありますのでご注意ください。●本製品はフレッツ光ネクスト、Bフレッツ、フレッツADSLで提供しているIPv6サービスには対応しておりません。●ウイルスブロック/迷惑メールブロックは本製品を経由するWeb、またはメール送受信に対して実施をいたします。●本製品は、外国為替および外国貿易法で定める規制対象貨物・技術に該当する製品です。この製品を輸出する場合または国外に持ち出す場合は、日本国政府の輸出許可が必要です。●本製品の補修用性能部品の最低保有期間は、製造打ち切り後7年です。●Windowsは、米国マイクロソフトコーポレーションの米国およびその他の国における登録商標です。●AndroidおよびAndroidロゴは、Google Inc.の商標または登録商標です。●AhkunおよびAntiMalwareは、株式会社アークンの商標または登録商標です。●Intel、Pentiumは、アメリカ合衆国およびその他の国におけるIntel Corporationの商標です。●その他の製品名および社名などは各社の商標または登録商標です。●仕様は予告なく変更する場合があります。●カラーは印刷の都合上、実際とは異なる場合があります。

saxa サクサ株式会社

本社/東京都港区白金1-17-3　NBFプラチナタワー　〒108-8050

■ソリューション営業統括本部

●オフィス営業本部
第一営業部 ☎(03)5791-5524
第二営業部 ☎(03)5791-3931

●交通・社会インフラ営業本部
第一営業部 ☎(03)5791-5853
第二営業部 ☎(03)5791-5531

●営業拠点
東北支社 ☎(022)297-5835　大宮営業所 ☎(048)650-9311
中部支社 ☎(052)220-3930　静岡営業所 ☎(054)653-7711
関西支社 ☎(06)6367-0393　金沢営業所 ☎(076)255-0393
九州支社 ☎(092)473-1511　高松営業所 ☎(087)861-7450
札幌営業所 ☎(011)281-1035　広島営業所 ☎(082)511-7555

●お客様相談室：0570-001393 ☎(050)5507-8039

URL http://www.saxa.co.jp/
E-mail customer@saxa-as.co.jp

●お問い合わせ・ご用命は

このカタログの記載内容は2012年7月現在のものです。

このカタログは再生紙を使用しております。

このカタログは植物油インキを使用しています。

SA-0310

サクサ UTM(統合脅威管理アプライアンス)

SS1000α

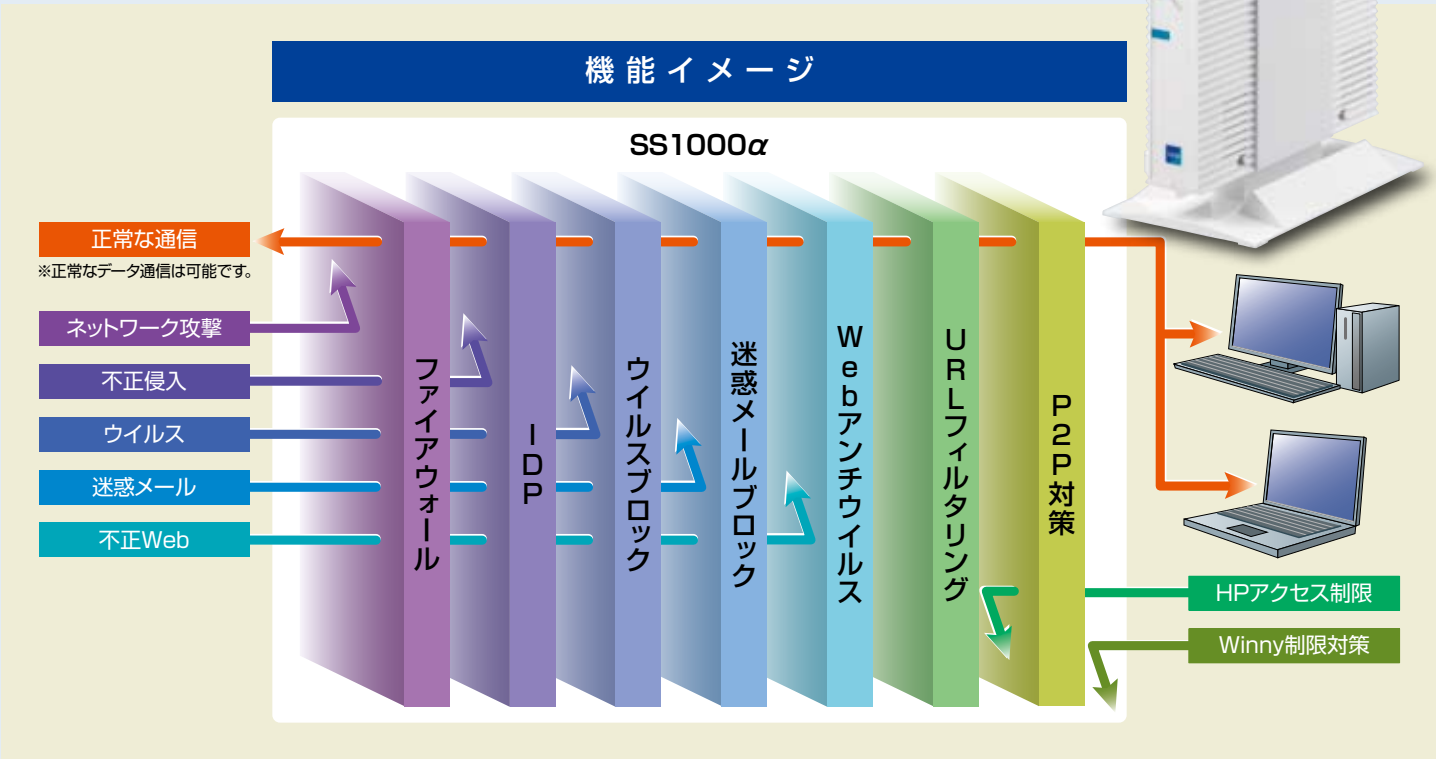
複数のセキュリティ機能を、1台の機器に集約!

ファイアウォール　IDP　ウイルスブロック　迷惑メールブロック　Webアンチウイルス　URLフィルタリング　P2P対策　ウイルス定義ファイルの5年間自動更新　ウイルス定義ファイルの6年間自動更新

悪意のある通信を遮断！
効果的なネットワークセキュリティを構築します。

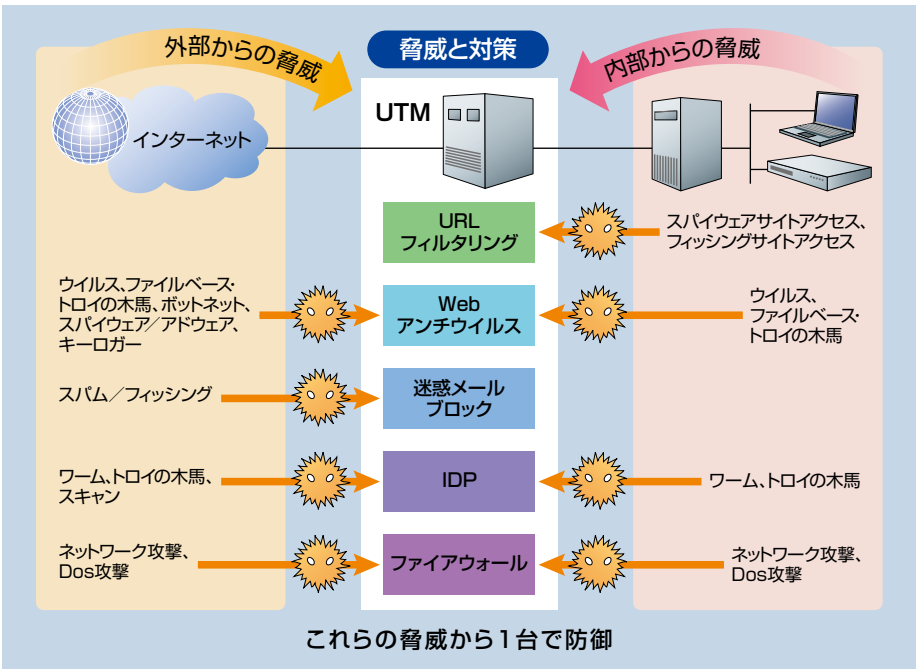
SS1000α[UTM]は、ファイアウォール、迷惑メールブロック機能、Webウイルス対策、メールウイルス対策、情報漏洩対策、不正侵入防御といった複数のセキュリティ機能を統合的に一元化。低コストでの導入･運用が可能な、オフィス向けのネットワークセキュリティ強化に最適な1台です。

■ウイルス定義ファイルの5年間自動更新、SS1000α Plusは6年間

■グラフィカルレポート
■駆動部品なしの高耐久性[ファンレス、ハードディスクレス]
■自動ファームウェアUP対応

UTM（統合脅威管理アプライアンス）とは

複数のネットワークセキュリティ技術を1台にパッケージ化。導入･運用･保守において大きなコスト削減のメリットがあります。

- ●ファイアウォール機能
- ●メールアンチウイルス機能
- ●Webアンチウイルス機能
- ●URLフィルタリング機能
- ●アンチスパム機能
- ●IDP
- ●P2P対策

脅威の種類	影　響
なりすまし	フィッシング
改ざん	システムファイルやアプリケーションの改変
否認	ユーザーの知らないうちに、電話やメールなどの通信やパケット通信を行う
漏洩	個人情報の漏洩（電話、メール、履歴、スケジュール、画像、動画など）
サービス拒否	断続的な着信拒否や、無線機能の停止、端末の異常停止など
権限昇格	Root権限の取得、システム権限の取得など

ファイアウォール機能

ファイアウォールとは、データ通信の状況や利用するソフトウェアなどにより、データをネットワークに通過させるか否かを判断し、不正なアクセスを防ぐことができる機能です。SS1000αを導入することにより、外部からの攻撃から社内ネットワークを守り、セキュリティを高めることができます。

IDP（侵入検出、防止）機能

IDPとは、Intrusion【侵入】Detection【検出】and Prevention【防止】の略で、社内ネットワークを外部の攻撃から守るための機能の総称です。SS1000αを導入することにより、インターネット上からのさまざまな攻撃に対し、社内ネットワークを守ることができます。

Webアンチウイルス機能

インターネット上には閲覧するだけでウイルス感染させる悪意あるホームページがあります。SS1000αを導入することにより、ホームページの閲覧時の通信を監視し、ホームページ上の画像や、ダウンロードするファイルにウイルスが混入していないかチェックを行いますので、パソコンへの侵入を防ぐことができます。

迷惑メールブロック機能

迷惑メールとは、不要なインターネット広告やウイルスが添付されたメールのことです。業務効率の低下を招いたり、偽造された銀行のホームページなどに誘導され、IDやパスワードを盗まれる危険性があります。SS1000αを導入することにより、迷惑メール（ウイルスが添付されたメールや特定のキーワードが記述されたメール）の対策が可能です。

URLフィルタリング機能

URLフィルタリング機能とは、あらかじめ指定したホームページへのアクセスを禁止する機能です。SS1000αを導入することにより、仕事に関係ないホームページ（オークションサイトや、掲示板サイト、日記共有サイト）へのアクセスを禁止することができるので、業務効率の低下を抑えることができます。

ネットワークの脅威

●情報漏洩
ウイルス･スパイウェア感染や不正アクセスにより、パソコン内の情報が外部へ漏洩。

●改ざん
不正アクセスにより、ホームページの内容やパソコン内の書類･データの不正な書換･削除。

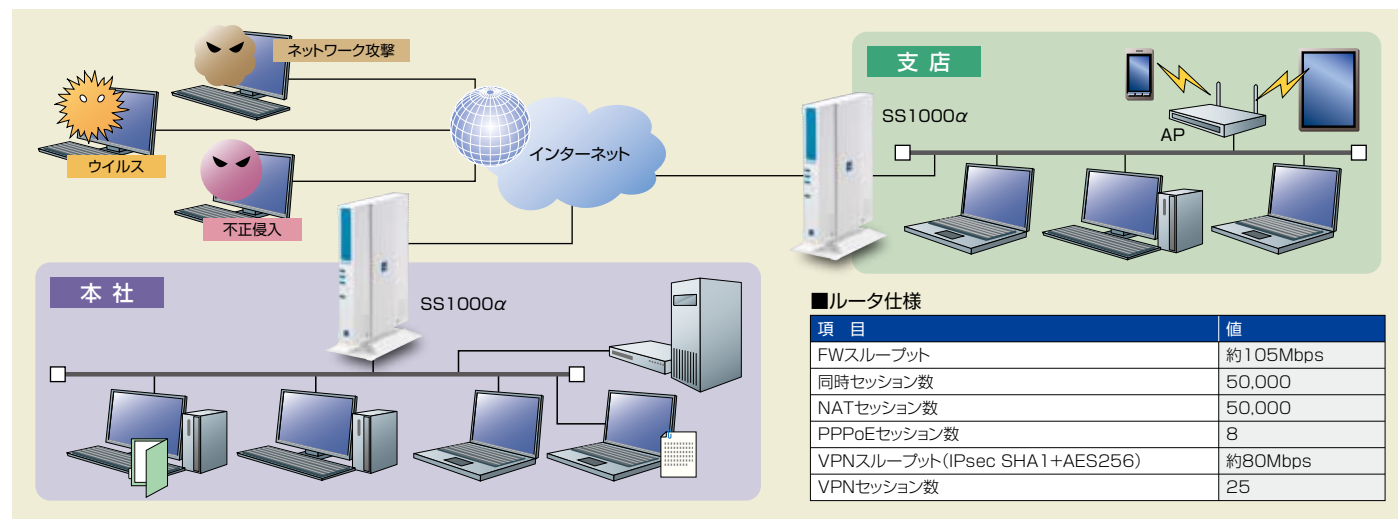
●なりすまし
銀行や有名企業を騙ったなりすましメールで偽サイトへ誘導し、IDやパスワードをだまし取る。

●サービス妨害
短時間に大量の通信を送りつけることで、動作を停止させ、サービスの提供を妨害する。

ルータ機能内蔵

ルータ機能が内蔵され、ネットワークの構築が容易になりました。また、IPSecによるVPNの構築も可能です。

■ルータ仕様

項目	値
FWスループット	約105Mbps
同時セッション数	50,000
NATセッション数	50,000
PPPoEセッション数	8
VPNスループット(IPsec SHA1+AES256)	約80Mbps
VPNセッション数	25

SS1000αログ解析ツール【見える化ツール】

見える化ツールを利用することにより、SS1000α導入の効果を視覚的に確認することができるようになります。
ログファイルは「メール」または「Web設定画面」から取得することができます。

見える化ツールの対応OS

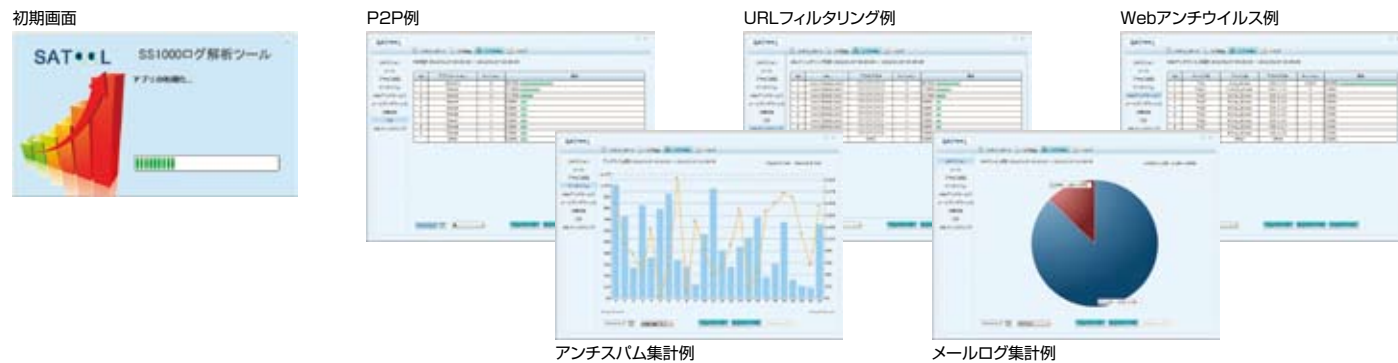
●Windows XP
●Windows Vista(32ビット版／64ビット版)
●Windows 7(32ビット版／64ビット版)

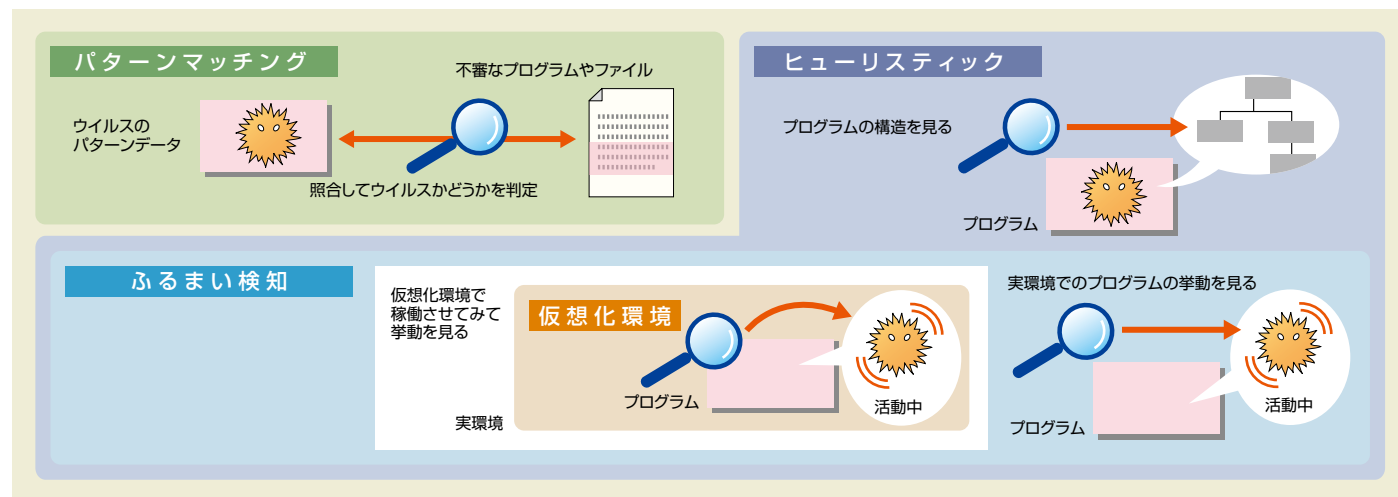
可視化できる内容

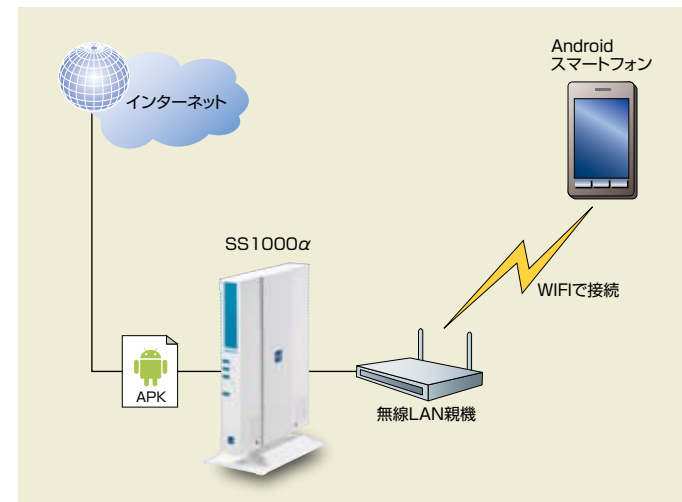
●コネクション　●メール　●アクセス拒否　●アンチスパム
●Webアンチウイルス　●メールアンチウイルス　●攻撃防御　●P2P
●URLフィルタリング　※表／棒／円でのグラフ化が可能です(一部を除く)。

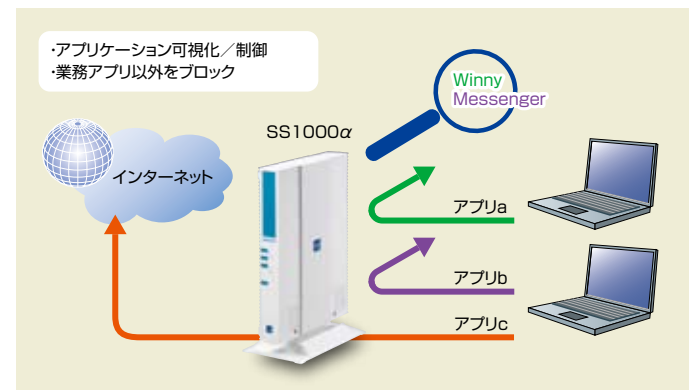
初期画面

P2P例　URLフィルタリング例　Webアンチウイルス例

アンチスパム集計例　メールログ集計例

不審な「ふるまい」検知対応(ヒューリスティック検知)

毎日誕生する多くの新種ウイルスに対して、定義ファイルによる検知方法だけでは対応することができません。ZEROデイ攻撃と呼ばれる対策パッチや定義ファイルが提供されるまでの間に攻撃されてしまうことを防ぐために、プログラムの不審な「ふるまい」を検知し、ウイルスと判断します。

スマートフォンセキュリティ対策

Android用パッケージファイル(APKファイル)のウイルスに対応しています。

P2P、メッセンジャーアプリの防御

P2Pとは、インターネットを介して、相手のパソコンと1対1で通信を行い、画像や映像ファイルの交換を行うソフトウェアのことです。SS1000αを導入することにより、P2P通信を遮断することができるので、セキュリティ対策を行っていない相手や悪意のある相手からのウイルス感染を防ぐことができます。

Ahkun AntiMalware-AV

エンドポイントセキュリティ

マルウェア(Malicious Software)とは、ウイルスはもちろん、不正侵入や情報漏洩につながるスパイウェアなどの不正プログラムやファイル交換ソフトなどです。これにより、迷惑メールの発信源にされたり大量のデータを送出して、プロバイダーから契約停止になる事例も増加しています。

ウイルス対策

高い検知力で、あらゆる侵入経路から、ウイルスの侵入を防ぎ、駆除します。

不正プログラム対策

ウイルス対策製品では見つかりにくい、スパイウェアなどのプログラムを検知、駆除します。

危険なプログラム対策

ファイル交換ソフトによる情報漏洩事件が後を絶ちません。8,000種以上のファイル交換ソフトを駆除します。

集中監視セキュリティ　「パソコン集中管理機能」

更新期日が過ぎていないか、最新のウイルスデータをアップデートしているか、検知したウイルスをきちんと処理しているかなどの煩わしい作業を管理者に代わってすべて自動で実行し、各クライアントパソコンをつねに最新のセキュリティレベルに保ちます。

USBセキュリティ　「挿入時オートスキャン機能」

USBメモリは手軽で便利なツールである反面、マルウェアを媒介させる危険なツールにもなります。ARCは、USBメモリの実行時に自動でスキャンし、問題があれば警告します。

内部統制セキュリティ　「パソコンの業務内容を日報形式で管理者へメール送信」

業務に無関係な操作を監視・抑止することがコンプライアンス上とても大切です。

●パソコンの利用時間統計
●パソコンの利用アプリケーション統計
●インターネットの閲覧履歴ログ
●プリントへの透かし印刷、利用制限
●プリンターの出力履歴ログ